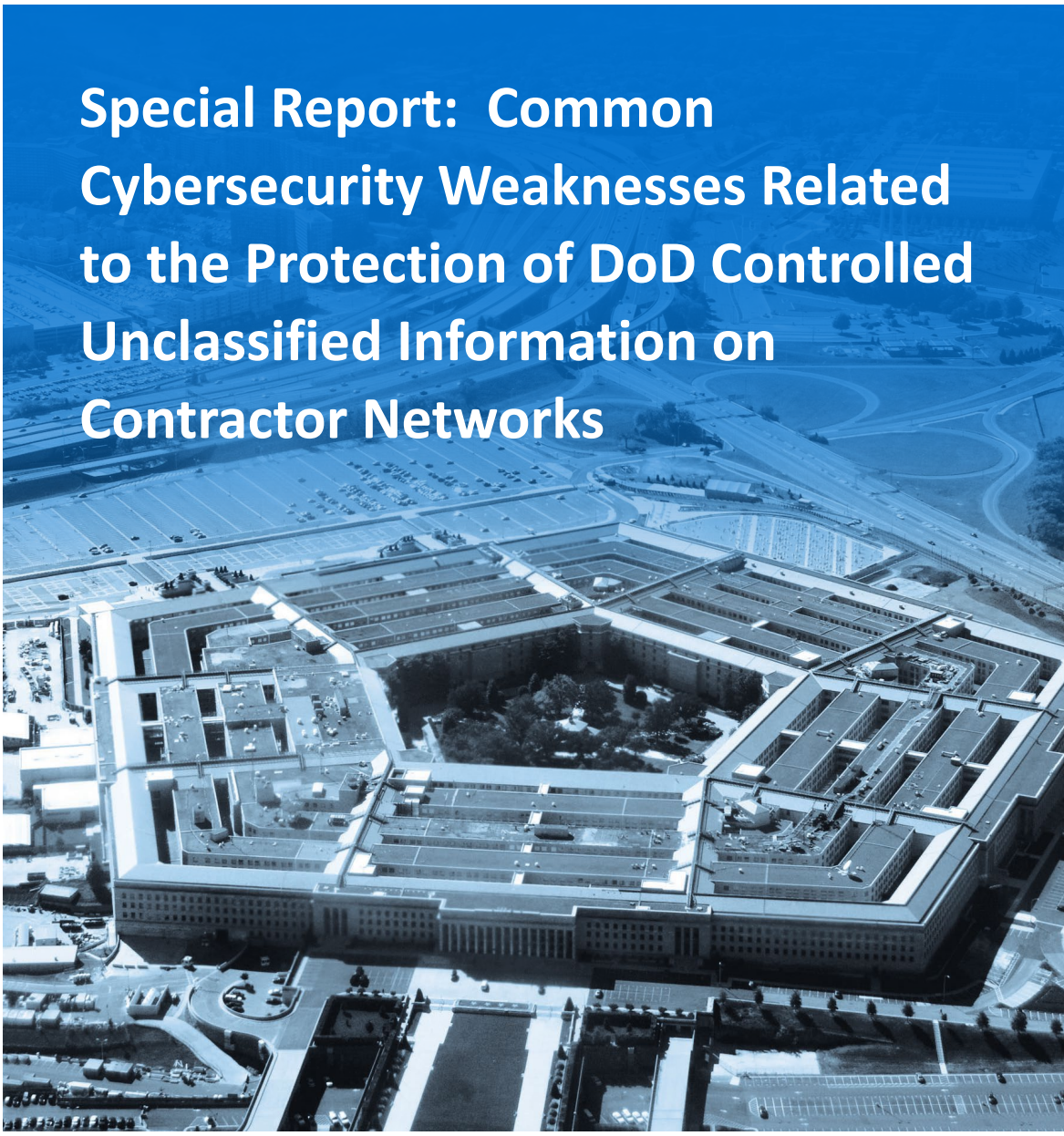
Report No. DODIG-2024-031

INSPECTOR GENERAL

U.S. Department of Defense

NOVEMBER 30, 2023

Special Report: Common Cybersecurity Weaknesses Related to the Protection of DoD Controlled Unclassified Information on Contractor Networks



INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

March 11, 2024

MEMORANDUM FOR DISTRIBUTION

SUBJECT: DoD Office of Inspector General Report No. DODIG-2024-031, "Special Report: Common Cybersecurity Weaknesses Related to the Protection of DoD Controlled Unclassified Information on Contractor Networks," November 30, 2023 (Report No. DODIG-2024-031)

We are revising two sentences on page 1 in the subject report to correct errors identified after publishing. The revisions are technical and do not affect the overall conclusions presented in the original report. You can find the updated report on our website at http://www.dodig.mil/reports.html.

We are revising the second sentence in the second paragraph, "DFARS 252.204-7012 requires contractors and grantees that maintain CUI to implement security controls specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800 171, which lists security requirements for safeguarding sensitive information on non Federal information networks and systems." to read, "Contractors and grantees that maintain CUI are required by DFARS 252.204-7012 and DoDI 8582.01, as applicable, to implement security controls specified in National Institute of Technology (NIST) Special Publication (SP) 800-171, which lists security requirements for safeguarding sensitive information on non-Federal information networks and systems." We are also revising the last sentence in the second paragraph "As of October 2016, DFARS 252.204-7012 is required in all DoD contracts and grants." to read, "As of October 2016, DFARS 252.204-7012 is required in all DoD contracts."

The report is a summary of previously issued audit reports and does not include findings and recommendations; therefore, we are not requesting comments on these revisions. As previously stated, the revisions do not impact the findings, conclusions, and recommendations of the summarized reports.

Please reference the attached page as a replacement page 1 for any copy of the subject report in your possession. We revised only the page indicated and modified no other information in the report.

If you have any questions on the revision, please contact me at [redacted] or [redacted].

FOR THE INSPECTOR GENERAL:

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

Attachment:
As Stated

Distribution:

SECRETARIES OF THE MILITARY DEPARTMENTS
UNDER SECRETARIES OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

Background

As of October 1, 2023, the DoD had 183,562 active contracts with organizations for goods and services that ranged from laboratory equipment and supplies to management support for weapon systems. To support the delivery of those goods and services, many DoD contractors process, store, and transmit controlled unclassified information (CUI) on their networks and systems.[1] CUI is information created or possessed for the Government that requires safeguarding or dissemination controls according to applicable laws, regulations, and Government-wide policies. CUI is not classified information as defined in Executive Order 13526, "Classified National Security Information," December 29, 2009. The responsibility of Federal agencies to protect CUI does not change when such information is shared with or used by contractors in the course of their contracts. Therefore, a similar level of protection is needed when CUI is processed, stored, or transmitted by contractors on their networks and systems.

The Defense Pricing and Contracting Office, a Component within the Office of the Under Secretary of Defense for Acquisition and Sustainment, establishes DoD contracting and procurement policy and provides updates to the Defense Federal Acquisition Regulation Supplement (DFARS), which requires contractors to safeguard DoD information.[2] Contractors and grantees that maintain CUI are required by DFARS 252.204-7012 and DoD Instruction 8582.01, as applicable, to implement security controls specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, which lists security requirements for safeguarding sensitive information on non-Federal information networks and systems.[3] As of October 2016, DFARS 252.204-7012 is required in all DoD contracts.

NIST SP 800-171 provides contractors with security requirements for protecting the confidentiality of DoD CUI. Specifically, contractors must implement or develop a plan to implement 110 security requirements to comply with NIST SP 800-171. The 110 security requirements are grouped into 14 categories that are defined in Table 1.

[1] An example of CUI is controlled technical information, or CTI. CTI is a category of CUI that includes technical information with military or space application that is subject to access, use, reproduction, modification, performance, display, release, disclosure, or dissemination controls.

[2] The Defense Pricing and Contracting Office was formerly known as the Defense Pricing Office and as the Defense Procurement and Acquisition Policy Office.

[3] DFARS Part 252, "Solicitation Provisions and Contract Clauses," Subpart 252.2, "Text of Provisions and Clauses," Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting.

DoD Instruction 8582.01, "Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information," December 9, 2019.

NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," Revision 1, December 2016 (Updated June 7, 2018).

Table 1. NIST SP 800-171 Security Requirements and Description

Security Requirement Category	Description
Access Control	The controls put in place to grant or deny user access to networks and systems and to the information that resides on those networks and systems.
Awareness and Training	Awareness is ensuring that users are aware of the security risks associated with their use of networks and systems and are aware of all applicable cybersecurity guidance. Awareness ensures users can recognize information system security concerns and respond accordingly. Training refers to the content and frequency of an organizations cybersecurity training and the efforts to ensure that all users attend the training.
Audit and Accountability	Audits are independent reviews and examinations to assess the adequacy of information system controls. Accountability is the principle that a user is trusted to safeguard and control information and must answer to the proper authority for the loss or misuse of the information.
Configuration Management	The process to document, review, and agree to baseline configuration settings and to maintain those settings over time and update the configuration settings based on security risks. Configuration settings are the parameters in software, hardware, or firmware that affect the security posture or functionality of a system. Settings can be defined in servers, workstations, input, and output devices and include settings for firewalls, wireless access points, sensors, and routers.
Identification and Authentication	The process of establishing and authenticating the identity of users that interact with networks and systems before granting access to the networks and systems.
Incident Response	The efforts to identify, report, analyze, contain, and mitigate internal or external network and system breaches or violations of security policies and recommended practices.
Maintenance	The activities to either prevent the failure or malfunction of networks and systems or to restore their operating capability. The activities include controls on the tools, techniques, and personnel used to conduct maintenance as diagnostic equipment and other maintenance tools could be potential vehicles for introducing malicious code into a system.
Media Protection	The process of restricting access or physically controlling media to ensure accountability, and restricting mobile devices capable of storing and carrying information into or outside of restricted areas. Media includes, but is not limited to, removable hard drives, flash drives, compact disks, and paper.
Personnel Security	The practice of assessing the conduct, integrity, judgment, loyalty, reliability, and stability of individuals for duties and responsibilities requiring trustworthiness.
Physical Protection	The practice of protecting and monitoring the physical facility and support infrastructure for networks and systems.
Risk Assessment	The process of identifying risks to organizational operations, assets, individuals, other organizations, and the Nation, resulting from the operation of networks and systems.

Table 1. NIST SP 800-171 Security Requirements and Description (cont'd)

Security Requirement Category	Description
Security Assessment	The testing or evaluation of security controls to determine whether the controls are implemented correctly, operating as intended, and producing the desired outcome to meeting the security requirements for networks and systems.
System and Communications Protection	The process of protecting the confidentiality and integrity of information at rest and in transit through physical and logical (automated) controls.
System and Information Integrity	The practice of monitoring networks and systems for security alerts, taking appropriate actions to address the alerts, and providing protection against malicious code.

Source: The DoD OIG.

When a prospective contractor responds to a DoD contract solicitation, the contractor must attest that they comply or will comply with the security requirements specified in the version of NIST SP 800-171 that is in effect at the time the solicitation is issued. Any deviation from NIST SP 800-171 requirements must be adjudicated (granted) by an authorized representative of the DoD Chief Information Officer before contract award. The contracting officer would work in coordination with the DoD Chief Information Officer to grant permission to deviate from the NIST SP 800-171 security requirements.

In October 2021, the Deputy Attorney General launched the Department of Justice's (DOJ) Civil Cyber-Fraud Initiative (CCFI). The CCFI combines the DOJ's expertise in civil fraud enforcement, government procurement, and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical networks and systems. Under the False Claims Act and through the CCFI, the DOJ pursues cybersecurity-related fraud by government contractors and grant recipients.[4] This includes holding accountable contractors who fraudulently attest on cybersecurity compliance self-assessments that security mechanisms were in place (or planned) to protect information that requires protection in accordance with DFARS 252.204-7012.

Individuals can file False Claims Act *qui tam* complaints, including suspected noncompliance with DFARS 252.204-7012, for investigation by the DOJ.[5] In addition to pursuing *qui tam* complaints, the DOJ uses Inspector General referrals, hotline complaints, whistleblower reporting, referrals from other Government organizations, and information about cyber incidents to initiate CCFI investigations into contractors.

[4] The False Claims Act, 31 U.S.C. §§ 3729 – 3733, states that any person who knowingly submits, or causes to submit, false claims is financially liable to the Government.

[5] A *qui tam* complaint allows private citizens to sue on behalf of the Government to recover money that was fraudulently obtained by a person or corporation.

Weaknesses Identified in DoD OIG Reports Related to Contractor Compliance with Cybersecurity Requirements for Protecting CUI

From 2018 through 2023, the DoD OIG issued five audit reports on DoD contractors' inconsistent implementation of the NIST SP 800-171 cybersecurity controls required by DFARS 252.204-7012 for protecting CUI. Those reports contained assessments of 29 DoD contractors providing products and services for 12 DoD Components. The five reports contained 116 recommendations to DoD Component contracting officers to ensure that the contractors corrected the weaknesses identified in the reports. Table 2 lists the five audit reports, the number of contractors assessed for each report, and the number of recommendations included in the reports specific to cybersecurity weaknesses.

Table 2. Audit Reports Concerning Contractor Compliance with NIST SP 800-171 Cybersecurity Controls by the Number of Contractors Assessed and Recommendations

Report Number, Title, and Issuance Date	Number of Contractors Assessed[1]	Number of Recommendations Specific to Cybersecurity Weaknesses[2]
DODIG-2023-078, "Audit of the DoD's Implementation and Oversight of the Controlled Unclassified Information Program," June 1, 2023	3	1
DODIG-2022-061, "Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors," February 22, 2022	10	18
DODIG-2020-098, "Audit of Governance and Protection of Department of Defense Artificial Intelligence Data and Technology," June 29, 2020	2	14
DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 23, 2019	10	80
DODIG-2018-094, "Logical and Physical Access Controls at Missile Defense Agency Contractor Locations," March 29, 2018	7	3

[1] We assessed three contractors across multiple audits.

[2] Some recommendations related to a specific cybersecurity weakness may have been addressed to multiple DoD Components responsible for overseeing selected contractors. For tracking purposes, we counted those recommendations separately (for example, if one recommendation listed five DoD Components, we tracked it as five recommendations).

Source: The DoD OIG.

In the five audit reports, we consistently determined that DoD contracting officials did not establish processes to verify that contractors complied with selected NIST SP 800-171 requirements.[6] Table 3 shows the systemic cybersecurity weaknesses that we identified across the five audits.

Table 3. Systemic Cybersecurity Weaknesses Identified During Audits of Contractor Compliance With NIST SP 800-171 Requirements

Systemic Cybersecurity Weakness and Associated NIST SP 800-171 Security Requirement Category	Audit Report				
	DODIG-2023-078	DODIG-2022-061	DODIG-2020-098	DODIG-2019-105	DODIG-2018-094
Networks and systems not configured to lock after a period of inactivity or unsuccessful log on attempts (Access Control)			X	X	X
System activity and user activity reports not generated and reviewed (Audit and Accountability)			X	X	X
Multifactor authentication or strong passwords not enforced (Identification and Authentication)		X	X	X	X
User accounts not disabled after extended periods of inactivity (Identification and Authentication)		X			
Physical security controls not used to detect unauthorized access (Physical Protection)		X	X	X	
CUI not protected on removable media (Media Protection)	X	X		X	X
Network and system vulnerabilities not identified or mitigated in a timely manner (Risk Assessment)		X	X	X	X
Networks and systems not scanned for viruses and malicious code (Risk Assessment)		X	X		

Source: The DoD OIG.

[6] To determine whether contractors had security controls in place to protect CUI stored on their information systems, we assessed certain security requirements that are especially critical to the protection of CUI.

As of October 2023, 24 recommendations related to contracting officials' oversight of contractor compliance with the cybersecurity requirements remain open, some of which have been open for as long as 4 years. See the Appendix for details on the 24 open recommendations.

Weaknesses Identified During CCFI Assessments Related to Contractor Compliance with Cybersecurity Requirements For Protecting CUI

In 2022, the DoD OIG began providing subject matter expertise to support the DOJ-led CCFI. Specifically, we reviewed third-party cybersecurity assessments, cyber incident reports, security policies, and system security plans to assist the DOJ in evaluating the contractor's compliance with NIST SP 800-171 requirements for protecting CUI. DoD OIG assessment results are used to support ongoing investigations of contractors who may have knowingly misrepresented their compliance with NIST SP 800-171 and to determine whether legal action should be pursued by the DOJ. Legal action may include treble damages and monetary penalties to reimburse the Government for losses incurred, up to $27,018 per false claim.[7]

As of October 2023, we have provided support for investigations of five DoD contractors under the CCFI. Table 4 shows the cybersecurity weaknesses and associated NIST SP 800-171 requirements that we identified during our CCFI assessments.

[7] Treble damages are when the court awards the plaintiff three times the amount of the actual damages.

Table 4. Cybersecurity Weaknesses Identified During CCFI Assessments

Cybersecurity Weaknesses and Associated NIST SP 800-171 Security Requirement Category	DoD OIG Assessment*				
	Assessment 1	Assessment 2	Assessment 3	Assessment 4	Assessment 5
Strong passwords not enforced (Access Control)	X			X	
Personnel access to facilities, networks, and systems are not controlled or monitored (Access Control, Personnel Security, and Physical Protection)	X	X	X	X	
Network, system, and user activity reports not generated and reviewed (Audit and Accountability)	X	X		X	X
Configuration settings are not monitored to detect deviations from configuration baselines or unauthorized software (Configuration Management)		X	X	X	X
User accounts not disabled after extended periods of inactivity (Identification and Authentication)	X	X	X		
Incident-handling not tracked, documented, or reported (Incident Response)	X	X		X	X
Network and system vulnerabilities not identified or mitigated in a timely manner (Risk Assessment)	X	X	X	X	X
Networks and systems not scanned for malware and malicious code (Risk Assessment)	X	X		X	X

* The investigations we supported are still ongoing; therefore, we cannot include information on specific contractors or the ultimate results.

Source: The DoD OIG.

Common Weaknesses Across DoD OIG Audit Reports and Civil Cyber Fraud Initiative Assessments

Comparisons of our findings on the five audits and the results of our CCFI assessments highlight a set of common cybersecurity weaknesses at DoD contractors that process, store, and transmit CUI related to access, audit and accountability, configuration management, identification and authentication, incident response, physical security, and risk management controls. While we did not select controls from all 14 NIST SP 800-171 cybersecurity categories in the audits or the CCFI assessments, the consistency of these common cybersecurity weaknesses across the audits and assessments provides DoD Component contracting officers, contracting officer's representatives, and contractors potential focus areas when assessing and ensuring compliance with NIST SP 800-171 cybersecurity requirements.[8] Table 5 summarizes the common cybersecurity weaknesses we identified in our audit reports and CCFI assessments.

Table 5. Summary of Common Cybersecurity Weaknesses Identified During Audits and CCFI Assessments

Cybersecurity Weakness	Summary
Multifactor Authentication or Strong Passwords	In four of the audits and two of the assessments, we identified that the contractors did not enforce the use of multifactor authentication or strong passwords. NIST SP 800-171 requires organizations to use multifactor authentication to access non-privileged network and system accounts. Multifactor authentication is authentication using two or more different factors to achieve authentication. Factors include something known to the user (for example, a personal identification number or password), something in the user's possession (for example, a cryptographic identification device or token), or a physical aspect of the user (such as biometric information). The use of multi-factor authentication reduces the risk of a security breach from compromised passwords. If multi-factor authentication is not used, NIST SP 800-171 requires the enforcement of a minimum password complexity requirement when using single-factor authentication. The use of complex passwords make it more difficult for malicious actors to guess the password.
System Activity and User Activity Reports	In three of the audits and four of the assessments, we identified that the contractors did not generate and review network, system, and user activity reports. NIST SP 800-171 requires organizations to generate audit records to allow for monitoring, analyzing, investigating, and reporting unauthorized system activity. Regular monitoring of user activity allows organizations to identify unauthorized access attempts and activity, help prevent breaches, and provide forensic evidence when investigating malicious behavior.

[8] The contracting officer's representative assists in the technical monitoring and administration of a contract and ensures that the contractor meets the commitments of its contract, including the timely delivery of quality goods and services.

Table 5. Summary of Common Cybersecurity Weaknesses Identified During Audits and CCFI Assessments (cont'd)

Cybersecurity Weakness	Summary
Disabling Inactive User Accounts	In one of the audits and three of the assessments, we identified that the contractors did not disable user accounts after an extended period of inactivity as required by NIST SP 800-171. Outdated or unused accounts provide network penetration points that may go undetected; therefore, inactive accounts should be disabled until needed, or removed.
Physical Security	In three of the audits and four of the assessments, we identified that the contractors did not implement physical security controls to monitor physical facilities containing their networks and systems. NIST SP 800-171 requires organizations to protect and monitor those physical facilities and provides examples of controls to include the use of video surveillance equipment such as cameras. Without physical security controls, security personnel have a limited capability to promptly identify and respond to security incidents and suspicious activities in and around the facilities.
Network and System Vulnerabilities	In four of the audits and five of the assessments, we identified that the contractors did not identify and mitigate network and system vulnerabilities in a timely manner. NIST SP 800-171 requires organizations to scan for vulnerabilities in their networks and systems and applications periodically, and develop plans of actions and milestones if they are unable to mitigate the vulnerabilities in a timely manner. If vulnerabilities remain unmitigated on an organizations network, malicious actors can exploit those vulnerabilities to gain access to the network. In addition, without a plan of action and milestones, contractors may be unable to correct network weaknesses, establish risk mitigation activities, or determine how long a vulnerability remained unmitigated on its network.
Scanning for Viruses and Malicious Code	In two of the audits and four of the assessments, we identified that the contractors did not scan networks and systems for viruses and malicious code. NIST SP 800-171 requires organizations to perform periodic scans of organizational networks and systems and real-time scans of files from external sources to detect malicious code. NIST SP 800-171 also requires system monitoring to include external and internal monitoring through a variety of tools and techniques including network monitoring software and scanning tools. Performing daily full-disk scans and updating virus definitions decreases the risk of missing opportunities to identify and mitigate emerging threats, such as malicious code contained within files.

Source: The DoD OIG.

Contractor compliance with NIST SP 800-171 requirements helps in reducing the risk of cyber-attacks and the loss of sensitive DoD data. The common cybersecurity weaknesses identified in this special report provide DoD contracting officers with potential focus areas when assessing contractor performance and DoD contractors and grant recipients with potential focus areas before assessing their compliance with NIST SP 800-171. These focus areas can also be considered when contractor assessments are conducted in accordance with DoD's "NIST SP 800-171 DoD Assessment Methodology." The DoD Assessment Methodology is designed to provide an objective opinion of the contractor's NIST SP 800-171 compliance status and can be required by the contracting officer before contract award and subsequently during the contract period.

Appendix

Open Recommendations Related to DoD Contractor Cybersecurity Weaknesses

In the five audit reports we discuss in this special report, we made 116 recommendations to DoD Components related to DoD contractor cybersecurity weaknesses. The following Figure shows the number of recommendations by security control category.

Figure. Recommendations by Security Control Category

Source: The DoD OIG.

As of October 1, 2023, 24 of the 116, or 21 percent of the recommendations remain open. Tables 6 through 8 list the:

- open recommendations by report;
- action offices responsible for resolving recommendations; and
- number of days the recommendations have been open.

To reduce the risk that DoD CUI is compromised, it is imperative that the DoD continue to take action to close the recommendations.

Report No. DODIG-2023-078, "Audit of the DoD's Implementation and Oversight of the Controlled Unclassified Information Program," June 1, 2023

Table 6. Status of Report No. DODIG-2023-078 Recommendations

Action Office	Recommendation	Number of Days Open as of October 2023
Under Secretary of Defense for Intelligence and Security	A.1.a. We recommend that the Under Secretary of Defense for Intelligence and Security, in coordination with the DoD Chief Information Officer and DoD Component Heads, develop and implement a DoD-wide solution for automatically populating documents and emails with the required markings based on a set of selection criteria.	122
Under Secretary of Defense for Intelligence and Security	A.1.b. We recommend that the Under Secretary of Defense for Intelligence and Security revise DoD Instruction 5200.48 to require DoD Components to implement a process to track the completion of CUI training, such as the use of a learning management system, and use that process to enforce the requirement that personnel complete the CUI training	122
Under Secretary of Defense for Intelligence and Security	A.1.c. We recommend that the Under Secretary of Defense for Intelligence and Security reissue notification to all DoD Component Heads that the Center for Development of Security Excellence controlled unclassified information training, "DoD Mandatory Controlled Unclassified Information (CUI) Training," is available on the DoD CUI website, and clarify that the training should be used for initial CUI training and can be also used as annual refresher training.	122
Under Secretary of Defense for Intelligence and Security	A.1.d. We recommend that the Under Secretary of Defense for Intelligence and Security add a question to the CUI questionnaire that requires DoD Components to select a sample of CUI documents, test whether personnel are including the required markings, and report the discrepancies identified during the test.	122
Under Secretary of Defense for Intelligence and Security	A.1.e. We recommend that the Under Secretary of Defense for Intelligence and Security coordinate with the National Archives and Records Administration to clarify the intent of the "Federal employees only" and "Federal employees and contractors only" limited dissemination controls, and when they should apply.	122
Under Secretary of Defense for Intelligence and Security	A.1.f. We recommend that the Under Secretary of Defense for Intelligence and Security revise DoD guidance to reflect any changes made to the use of the "Federal employees only" and "Federal employees and contractors only" limited dissemination controls.	122

Table 6. Status of Report No. DODIG-2023-078 Recommendations (cont'd)

Action Office	Recommendation	Number of Days Open as of October 2023
Under Secretary of Defense for Intelligence and Security	A.1.g. We recommend that the Under Secretary of Defense for Intelligence and Security develop and implement a process to identify systemic discrepancies with the implementation of CUI programs across the DoD Components and provide guidance to the DoD Components to address those systemic issues.	122
Under Secretary of Defense for Intelligence and Security	A.1.h. We recommend that the Under Secretary of Defense for Intelligence and Security require DoD Components that identify discrepancies within their CUI program to develop and implement corrective action plans, and provide updates on the actions taken to resolve the discrepancies in future years questionnaires.	122
Department of the Army	A.2. We recommend that the Commanding General of the Army Training and Doctrine Command update the Training Development Capability to include the option to mark documents as CUI and prompt personnel to add the designation indicator and portion markings, if applicable.	122
Department of the Navy	A.3. We recommend that the Chief of Naval Operations update standard forms and templates to include CUI headers and footers, and prompt personnel to add the designation indicator and portion markings.	122
Department of the Air Force	A.4. We recommend that the Director of Information Management, Office of the Administrative Assistant to the Secretary of the Air Force, update standard forms and templates to include CUI headers and footers, and prompt personnel to add the designation indicator and portion markings.	122
Defense Pricing and Contracting	B.1.a. We recommend that the Defense Pricing and Contracting Principal Director direct DoD contracting officers for contracts that involve CUI to verify that contractor-developed controlled unclassified information training includes the 11 DoD learning objectives as outlined in DoD Instruction 5200.48 and that the contractors have established a process to maintain documentation of completed training for audit purposes.	122
Defense Pricing and Contracting	B.1.b. We recommend that the Defense Pricing and Contracting Principal Director coordinate with the Office of the Under Secretary of Defense for Intelligence and Security and the DoD Chief Information Officer to develop a Defense Federal Acquisition Regulation Supplement clause to require all DoD contractor personnel to complete the required DoD CUI training.	122
Missile Defense Agency	B.2. We recommend that the Missile Defense Agency contracting officer require Contractor C to establish a process to maintain documentation of completed CUI training for audit purposes.	122

Source: The DoD OIG.

Report No. DODIG-2022-061, "Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors," February 22, 2022

Table 7. Status of Report No. DODIG-2022-061 Recommendations

Action Office	Recommendation	Number of Days Open as of October 2023
Department of the Navy	3.b. We recommend that the Commander of the Naval Sea Systems Command direct contracting officers to verify that the contractor enforces multifactor authentication; disables user accounts after extended periods of activity; implements technical security controls to protect CUI stored on removable media; and implements physical security controls.	586
Department of the Navy	3.c. We recommend that the Commander of the Naval Sea Systems Command direct contracting officers to verify that the contractor enforces multifactor authentication; encrypts CUI stored on workstations; and implements technical security controls to protect CUI stored on removable media.	586
Under Secretary of Defense for Research and Engineering	5.b. We recommend that the Director of Defense Research and Engineering for Research and Technology direct contracting officers to verify that the contractor identifies and mitigates vulnerabilities and develops plans of action and milestones for vulnerabilities that cannot be mitigated in a timely manner; encrypts CUI stored on workstations; and implements technical security controls to protect CUI stored on removable media.	586

Source: The DoD OIG.

Report No. DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 23, 2019

Table 8. Status of Report No. DODIG-2019-105 Recommendations

Action Office	Recommendation	Number of Days Open as of October 2023
DoD Chief Information Officer	A.1.a. We recommend that the DoD Chief Information Officer, in coordination with Defense Pricing and Contracting, implement or revise policy to require all systems and networks that maintain DoD information, including those owned by contractors that maintain DoD information to use strong passwords that, at a minimum, meet DoD password length and complexity requirements.	1,531
DoD Chief Information Officer	A.1.b. We recommend that the DoD Chief Information Officer, in coordination with Defense Pricing and Contracting, implement or revise policy to require all systems and networks that maintain DoD information, including those owned by contractors that maintain DoD information to configure their systems and networks to align with DoD requirements for locking after 15 minutes of inactivity and 3 unsuccessful logon attempts.	1,531
Defense Pricing and Contracting	A.2.a. We recommend that the Principal Director for Defense Pricing and Contracting, in coordination with the appropriate DoD Component responsible for developing policy, revise its current policy to require DoD Component contracting offices, as part of the Request for Proposal and source selection processes, and requiring activities, during the performance of the contract, to assess whether contractors comply with NIST requirements for protecting CUI before contract award and throughout the contracts' period of performance.	1,531
Defense Pricing and Contracting	A.2.b. We recommend that the Principal Director for Defense Pricing and Contracting, in coordination with the appropriate DoD Component responsible for developing policy, develop and implement policy requiring DoD Component contracting offices and requiring activities to maintain an accurate accounting of contractors that access, maintain, or develop CUI as part of their contractual obligations.	1,531
Defense Pricing and Contracting	A.2.c. We recommend that the Principal Director for Defense Pricing and Contracting, in coordination with the appropriate DoD Component responsible for developing policy, revise its current policy to include language that will require DoD Component contracting offices and requiring activities to validate contractor compliance with NIST SP 800-171 requirements.	1,531

Table 8. Status of Report No. DODIG-2019-105 Recommendations (cont'd)

Action Office	Recommendation	Number of Days Open as of October 2023
Defense Pricing and Contracting	A.2.d. We recommend that the Principal Director for Defense Pricing and Contracting, in coordination with the appropriate DoD Component responsible for developing policy, require DoD Component contracting offices, in coordination with DoD requiring activities, to develop and implement a risk-based process to verify that contractors comply with the DFARS clause 252.204-7012 for protecting CUI.	1,531
Defense Pricing and Contracting	A.2.e. We recommend that the Principal Director for Defense Pricing and Contracting, in coordination with the appropriate DoD Component responsible for developing policy require DoD Component contracting offices, in coordination with DoD requiring activities, to take corrective actions against contractors that fail to meet the NIST and contract requirements for protecting CUI.	1,531

Source: The DoD OIG.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098